Diplomasi ve Strateji Dergisi
The Journal of Diplomacy and Strategy

Yıl/Year: 2022

Cilt/Volume: 3
Sayı/Issue: 2

Makale Geliş Tarihi: 14/10/2022 **Makale Kabul Tarihi: 14/01/2023**

ULUSAL GÜVENLİK AÇISINDAN KRİTİK ALTYAPI VE SİBER ALAN: SİVİL HAZIRLIKLILIK VE DİRENÇLİLİK PERSPEKTİFİNDEN KAVRAMSAL BİR İNCELEME

Aybike CAN[1]

Öz

Ulusal güvenlik, askeri kapasite kadar askeri olmayan unsurların da savunmaya katılmasını ifade etmektedir. Bireylerin, özel sektörün, kritik altyapının, kentlerin ve siber alanın dirençliliği sivil savunmanın ilk basamağını oluşturmaktadır. Dirençlilik, sayılan unsurların topyekûn hazırlıklılığı anlamına gelmektedir. AB ve NATO güvenlik tanımlarında dirençliliği yeni bir konsept olarak kabul etmiştir.

Bu çalışmada kritik altyapının ve siber alanın dirençliliğinin ulusal güvenlik üzerindeki yansımasını belirlemek amaçlanmıştır. Çalışma nitel bir çalışma olup ilgili içerik literatürden derlenmiştir. Konu, güvenlik ve terör çalışmalarında görece yeni bir konsept olan sivil hazırlıklılık ve dirençlilik kavramları perspektifinden araştırılarak literatürdeki bu alandaki boşluk giderilmeye çalışılmıştır.

İlk bölümde kavram analizi yapılarak kavramlar tanımlanmış, unsurları belirlenmiştir. İkinci bölümde kritik altyapılar ve kritik altyapıların dirençliliği incelenmiştir. Üçüncü bölümde ise siber dirençlilik ele alınmıştır. Çalışmada terör saldırıları, KBRN saldırıları ve savaşlarda doğrudan siber alanın ve kritik altyapının hedeflendiği dolayısıyla bu alanlarda dirençliliği artırmanın ulusal güvenlik sorunu olduğu sonucuna ulaşılmıştır. Kritik altyapının ve siber alanın dirençliliğinin

[1] Dr.
aybike.can@hotmail.com
ORCID: 0000-0001-5587-7385

bireyler, özel sektör ve devlet kuruluşlarının hazırlıklı olmasına ve işbirliğine dayalı olduğu ulaşılan sonuçlardan bir diğeridir.

Anahtar Kelimeler: *Sivil Hazırlıklılık, Dirençlilik, Kritik Altyapı, Siber Güvenlik, Sivil Savunma.*

CRITICAL INFRASTRUCTURE AND CYBERSPACE FOR NATIONAL SECURITY: A CONCEPTUAL INVESTIGATION FROM THE PERSPECTIVE OF CIVIL PREPAREDNESS AND RESISTANCE

Abstract

National security refers to the participation of non-military elements in defense as well as military capacity. The resilience of individuals, the private sector, critical infrastructure, cities and cyberspace constitutes the first step of civil defense. Resilience means the total preparedness of the counted elements. The EU and NATO accept resilience as a new concept in their security definitions.

In this study, it is aimed to determine the reflection of the resilience of critical infrastructure and cyberspace on national security. The study is a qualitative study and the relevant content was compiled from the literature. The subject has been investigated from the perspective of the concepts of civil preparedness and resilience, which are a relatively new concept in security and terrorism studies, and the gap in this field in the literature has been tried to be filled.

In the first part, concepts were defined by making concept analysis and their elements were determined. In the second part, critical infrastructures and resilience of critical infrastructures are examined. In the third part, cyber resilience is discussed. In the study, it was concluded that cyber space and critical infrastructure are directly targeted in terrorist attacks, CBRN attacks and wars, so increasing resilience in these areas is a national security problem. Another result is that the resilience of critical infrastructure and cyberspace is based on the preparedness and cooperation of individuals, private sector and government organizations.

Keywords: *Civil Preparedness, Resilience, Critical Infrastructure, Cyber Security, Civil Defence.*

Giriş

Modern toplumların gücü, askeri kaynaklarının yanı sıra stratejik ve kırılgan varlıklarının dayanıklılığı ve sivil toplumun dirençliliği ile doğru orantılıdır. Herhangi bir tehdit veya olası savaş durumunda askeri unsurların desteklenmesi ve sürdürülebilirliği o toplumun kaderini belirlemektedir. Nitekim olası bir terör saldırısı, silahlı çatışma, doğal afet, büyük çaplı kaza veya diğer hibrit tehditler sonrasında hızlı bir toparlanma sürecine girilmesi büyük önem taşımaktadır. Yine bir kriz anında devlet organlarının desteklenmesi ve bu organların görevlerini yerine getirebilmesi de elzemdir. Bütün bu belirtilen senaryolar, askeri unsurlar kadar askeri olmayan unsurların da savunmaya katılma yönünde hazırlıklı olmasını gerekli kılmaktadır. Herhangi bir saldırı karşısında bireysel ve toplu direnme kapasitesi, sivil dirençlilik olarak adlandırılmaktadır.

Günümüzde devletler ve toplumlar daha kapsamlı ve değişik nitelikte tehdit ve saldırılarla karşı karşıya kalmaktadırlar. Hibrid tehditler olarak adlandırılan bu saldırılar basit sosyal medya saldırılarından siber saldırılara, seçim süreçlerini sabote etmekten yanlış haber yaymaya, ekonomik manipülasyona veya açıkça silahlı kuvvet kullanımına kadar değişmektedir. Bu yöntemlerden bir veya birkaçının bir arada kullanılması da mümkündür. Hibrit nitelikli saldırılar, konvansiyonel ve konvansiyonel olmayan, askeri ve askeri olmayan taktik ve araçların kullanıldığı saldırıları ifade etmektedir. Devletler veya devlet dışı aktörler tarafından yönlendirilebilirler. Terör örgütleri ve organize suç örgütleri arasındaki ayrımın bulanıklaşması da devletlerin karşılaştığı tehditlerin çeşitlenmesine yol açmıştır. Hibrit tehditler sürekli değişen ve teknolojik gelişmelerle birlikte çeşitlenen

nitelikte olup hedeflerin zayıf noktalarına yönelik olarak hazırlanırlar. Bu durum devletlere kendisine yönelebilecek tehditleri belirleyebilme imkanı da sağlamaktadır. Devletler hedef konumunda olabilecek yapıları ve sosyolojik unsurları önceden belirleyerek hazırlıklı olmalı ve güvenlik açıklarını kapatmalıdırlar (Hagelstam 2018; Dupuy vd. 2021).

Hibrit tehditler, olası Kimyasal Biyolojik Radyolojik Nükleer (KBRN) saldırılar, kamusal alanlara yönelik saldırılar, diğer terör eylemleri, depremler, yangınlar ve halk sağlığını tehlikeye atacak salgınlar karşısında ulusal, bölgesel ve uluslararası ölçekte hazırlıklılık ve işbirliği gerekmektedir. Belirtilen tehdit ve afetlerin çok yönlü doğası, hazırlıklılık ve dirençlilik plan ve çalışmalarında bireyin, ailenin, özel işletmelerin, devlet kurumlarının yer alması gerektiğini ortaya çıkarmaktadır. Hazırlıklılığın dayanması gereken ve tüm devlet ve tüm toplum yaklaşımı (whole of government/society) olarak da anılan bu işbirliği, kriz, saldırı ve doğal afet anlarında ulusal dirençlilik için gerekli görülmektedir (Wigell, Mikkola ve Juntunen 2021, 21). Tüm toplumun işbirliği içerisinde hazırlıklı olması, AB, NATO ve diğer uluslararası kuruluşların da benimsediği hazırlıklılık ve dirençlilik perspektifini oluşturmaktadır.

Bu çalışmada literatür taraması yapılarak kritik altyapının ve siber alanın dirençliliğinin ulusal güvenlik üzerindeki etkilerini belirlemek amaçlanmıştır. Çalışma nitel bir çalışma olup, çalışmanın kavramsal çerçevesini dirençlilik ve hazırlıklılık kavramları oluşturmaktadır. Güvenlik çalışmalarında görece yeni bir konsept olan dirençlilik ve hazırlıklılık perspektifinden kritik altyapı ve siber alanın ele alınması, literatüre katkı niteliğinde olacaktır.

Çalışmada ilk olarak dirençlilik ve hazırlıklılık kavramları tanımlanacak ve unsurları belirlenecektir. Ardından ikinci başlık altında kritik altyapı kavramı ve kritik altyapının dirençliliği incelenecektir. Çalışmanın üçüncü bölümünde siber dirençlilik kavramı ele alınacaktır. Çalışmada kritik altyapı ve siber alanın dirençliliği ve hazırlığının ulusal güvenlik için elzem olduğu sonucuna ulaşılmıştır. Kritik altyapı ve siber alanın dirençliliğinin sağlanmasının tüm toplum yaklaşımı çerçevesinde bireysel ve kurumsal hazırlık ve işbirliğini gerektirdiği ulaşılan sonuçlardan bir diğeridir.

1. Dirençli Toplum ve Sivil Hazırlıklılık

Bir ülkenin dirençli olması için askeri gücünün yanı sıra terör saldırısı, KBRN saldırıları veya doğal afetlere karşı bireyin, toplumun, özel sektörün ve devletin topyekûn hazırlıklı olması gerekmektedir. Tehditlerin değişen ve çeşitlenen doğası, dirençliliğin tüm toplum ve tüm devlet yaklaşımıyla ele alınmasına yol açmıştır. Buna göre, dirençlilik katmanlar halinde ele alınması ve bu katmanlar arasında işbirliği ve uyumun olması gereken bir kavramdır. Özel sektör ve sivil toplum aktörlerinin tüm kapasite ve varlıklarıyla stratejik planlama sürecine katılması gerekmektedir. Tüm toplum yaklaşımıyla dirençliliğin sağlanması sürecinde dört katman bulunduğu varsayılmaktadır. İlk katman bireysel dirençlilik olup bireylerin psikolojik yeterlilikleri göz önüne alınmaktadır. Bireysel dirençliliği artırmak için toplumdaki eşitsizlikleri azaltacak sosyal politikalar ve eğitim süreçleri takip edilmelidir. Dirençliliğin ikinci katmanı topluluk (community) bazındaki dirençlilik olup yaşanılan topluluktaki birlik ve beraberlik duygusunun gelişmesini ifade etmektedir. Üçüncü katman kurumsal dirençlilik olup sosyal politikalar, kritik altyapıların

planlanması ve karar alma mekanizmasının işlerliğine atıf yapmaktadır. Dirençli toplum için bu aşama kritik olup eğitim ve refahın tüm topluma yayılması temeldir. Bu aşamada hibrit tehditler arasında yer alan seçimlere hile karıştırılması ve dezenformasyon kampanyalarının önlenmesi yer almaktadır. Dirençliliğin dördüncü katmanı, dış ilişkiler, işbirlikçi yapı ve kurumsal düzenlemelerden oluşmaktadır. Bu aşamada tedarik zincirinin planlanması ve güvenliği için uluslararası işbirliği gibi düzenlemeler yer almaktadır (Wıgell, Mıkkola ve Juntunen 2021, 22). Görülebildiği üzere dirençlilik bireyler, özel işletmeler, kurumlar, yasal düzenlemeler ve uluslararası işbirliği ile tüm toplumun hazırlıklı olmasını gerektirmektedir.

Etkin bir hazırlıklılık için tehdit öncesinde ve sırasında yapılacaklar önceden belirlenmeli, tehdit geçtikten sonra toparlanma süreci önceden planlanmalıdır. Bu sebeple öncelikle mikro düzeyde farkındalık oluşturmak, eğitimler vermek, tatbikatlar yapmak gerekmektedir. Makro seviyede ise devletin fiziki veya sosyolojik kırılgan unsurları ve riskleri belirlemesi gerekmektedir. Devlet, özel sektör temsilcileriyle de işbirliği içerisinde olmalıdır. Böylelikle tehdit sona erdiğinde sistemin hızlıca yeniden işlerlik kazanması amaçlanmalıdır.

1.1. Dirençliliği Tanımlamak

21. yüzyılda toplumların kırılgan, belirsiz ve kesinlikten uzak doğası, savunma konusunda yeni anlayışlar belirlenmesini gerekli kılmıştır. Çatışmaların değişen doğası ve modern dünyadaki çatışmaların devlet ve toplumun tüm unsurlarını hedef olarak belirleyebilmesi sivil hazırlıklılık yoluyla dirençliliği ön plana

çıkarmıştır. Dirençlilik, sivil hazırlıklılık ve askeri kapasitenin birleşimi olarak değerlendirilmektedir. Dirençlilik toplumun büyük şok, doğal afet, terör saldırısı veya askeri saldırı karşısında direnme yeteneğini ve ardından yaralarını hızlıca sarma ve iyileştirme yeteneğini de kapsamaktadır. Dirençliliği yüksek bir devlet veya toplum, olası saldırılar bakımından daha düşük bir hedef olacaktır (CCOE t.y.).

Değişim ve dönüşüm anlamlarıyla değerlendirildiğinde dirençlilik, ortaya çıkan yeni durumu anlama, kendini değiştirme ve dönüşüme uyum sağlama olarak tanımlanabilecektir. Literatürde dirençliliğin birden fazla türünün olduğu görülmektedir. Örneğin kurumsal dirençlilik yönetim, yönetim yapısı, hükümet, bürokratik ve örgütsel yapının direncini anlatmaktadır. Ekonomik dirençlilik toplumdaki işgücü verilerinin, istihdam oranının olası bir krize karşı koyabilme ve kriz sonrasında toparlanabilme kapasitesini ifade etmektedir. Altyapı direnci ulaşım, enerji santralleri, iletişim hatları vb. gibi inşa edilen yapıların kırılganlığının azaltılması anlamına gelmektedir (Ersavaş Kavanoz 2021, 386).

Mikro anlamda dirençlilik bireylerin fiziksel, zihinsel ve ruhsal sağlamlığını anlatmaktadır. Bireysel dirençlilik kişilik özellikleri, sosyal bağlar ve sorun çözme becerilerini içermektedir. Eğitim durumu, ailevi özellikler ve sosyal çevre kişinin bireysel direncini etkilemektedir. Kişilerin iyimserlik, kişisel yeterlilik, uyum gibi karakter özellikleri, herhangi bir acil durum anında ve sonrasında psikolojik olarak dirençli olmalarını sağlamaktadır. Kişilerin sosyal bağları, onların kaynaklara ve topluluk desteğine ulaşmalarını kolaylaştıracaktır. Son olarak sorun çözme becerileri ve başa çıkma stratejileri bireysel direnci artıracaktır (Kindt 2006, 6; Varol ve

Kırıkkaya 2017, 2).

Otoriteler acil durum planlaması yaparken kriz anlarında bireysel direnci etkileyen özellikleri göz önünde tutmalıdırlar. Bunun için psikoloji, sosyoloji, sosyal psikoloji gibi disiplinlerden faydalanılmalıdır. Örneğin Kindt (2006, 9), bireylerin herhangi bir kriz anında güvenli alanlara yönelmek yerine tanıdığı insanlar ve tanıdığı yerlere yönelme eğiliminde olduklarına işaret etmektedir. Tanınan kişi ve yerlerden ayrılmak kişiler üzerinde afet ve tehditin yol açacağından daha fazla zarara yol açabilmektedir. Ona göre, şok ve krizler sırasında panik yaşanmamasının yolu sosyal kontrol ve baskı değil, insanların aşina oldukları kişilerden ayrılmamasıdır. Bireylerin doğal afet ve kriz anlarında gösterme eğiliminde oldukları davranışların araştırılması, doğru veya hatalı davranışların afetlere hazırlık eğitimiyle bireye öğretilmesi açısından da önemlidir. Örneğin deprem anında kaçma dürtüsü insanlarda genel bir eğilimken, eğitimlerle bunun doğru olmadığı insanlara aşılanabilecek ve kriz anında doğru davranışta bulunma yetisi tatbikatlarla kazanılabilecektir.

Makro anlamda dirençlilik ise sosyal dirençlilik veya toplumsal dirençlilik olarak isimlendirilmektedir. Sosyal dirençlilik, bir topluluğun şoklara ve krizlere karşı dayanma gücü olarak tanımlanabilmektedir. Sosyal-toplumsal direncin dört farklı değişkeni olduğu belirtilmektedir. Bunlar ekonomik kalkınma, sosyal - beşeri sermaye, enformasyon ve iletişim kapasitesi ile kolektif eylem için topluluk becerisidir (Norris vd. 2008, 136). Sosyal dirençlilik toplumun eğitim, sosyo-ekonomik statü, yaş vb. özelliklerine ve topluluk bağlarının güçlülüğüne atıf yapmaktadır.

Dirençlilik son dönemlerde terörle mücadele literatüründe sıklıkla kullanılmaya başlanmıştır. Terörizm çalışmalarında dirençlilik, bir sistemin veya sosyal birimin direnme kapasitesi ve içsel veya dışsal bir şoktan sonra toparlanma kapasitesi olarak tanımlanmaktadır. Terörle mücadelede dirençlilik konsepti, teröristlerden gelebilecek karmaşık tehdit ve tehlikeleri önceden belirleyebilmeyi ve bunlara cevap verebilmeyi içermektedir. Terörle mücadelede dirençlilik yaklaşımı, terör saldırısına hedef olabilecek kalabalık kamusal alanların hedef olma olasılığını azaltmayı ve olası bir saldırıda karşılık verebilmeyi içermektedir (Coaffee 2009, 263, 276). Dirençlilik bir sosyal birimin veya sistemin ilk şoktan sonra orijinal durumuna dönebilmesini veya kendisini daha önce olduğundan daha güçlü bir şekilde iyileştirerek inşa etmesini sağlamaktadır. Terörist saldırının ardından yaralarının sarılabilmesi, vatandaşların, kurumların, toplumun ve sistemin tekrar eski durumuna ve işlerliğine dönebilmesi amaçlanmalıdır. Dolayısıyla dirençlilik toplumların, kurumların, organizasyonların ve bireylerin terörle mücadele stratejilerini nasıl şekillendirmeleri gerektiği konusunda yol gösterici bir kavram haline gelmiştir (Jore 2020, 1). Teröre karşı dirençliliğin önemli bir yönünü de psikolojik dirençlilik oluşturmaktadır. Çünkü terör kelime anlamı olarak korku salmak, halkta panik uyandırmak anlamlarına gelmektedir. Psikolojik dirençliliği kırmak için terör gruplarının sosyal medyayı sıklıkla kullandığı ve yalan haberler yaydığı görülmektedir. Vatandaşların herhangi bir saldırı sırasında ve sonrasında doğru şekilde bilgilendirilmesi, güvenilir kaynaklardan bilgi akışı sağlanması kritik önem taşımaktadır.

Dirençlilik çok boyutlu bir süreç olup psikolojik, davranışsal ve

fiziki boyutlarıyla düşünülmelidir. Kavram sosyoloji, iktisat, mühendislik, mimari, halk sağlığı, psikoloji, kamu yönetimi ve acil durum yönetimi gibi pek çok disiplinin yardımıyla topyekün bir hazırlıklılığı ifade etmektedir (Varol ve Kırıkkaya 2017, 8). Bu kapsamda devlet ve toplum bütünlüğü perspektifiyle kentlerin hazırlıklılığı, bireylerin hazırlıklılığı, binaların hazırlıklılığı, altyapının hazırlıklılığı, yönetimin hazırlıklılığı, özel sektörün hazırlıklığı vb. aşamaların hepsi dirençliliğin birer parçası haline gelmektedir. Dirençliliğin bu çok boyutlu yönü planlama, strateji, eğitim ve tatbikat aşamalarının hepsinde geniş halk katılımını gerekli kılmaktadır. Dirençlilik ancak risk, tehdit ve tehlikeleri çok yönlü olarak belirleyip bunlara hazırlıklı olmakla sağlanabilecektir. Aşağıdaki başlık altında dirençliliği sağlamanın yolu olarak hazırlıklılık kavramı ele alınacaktır.

1.2. Dirençliliği Sağlamanın Yolu Olarak Hazırlıklılık

Sivil hazırlıklılık herhangi bir kriz durumunda, terör ve KBRN saldırısında veya doğal afette toplum için hayati fonksiyonların devamını, halka temel ihtiyaç ve hizmetlerin ulaştırılabilmesini, devletin fonksiyonlarını devam ettirebilmesini, hükümet ve devlet kurumlarının işlerliğini ve askeri operasyonlara sivil desteğin sağlanmasını ifade etmektedir. Sivil hazırlıklılık kavramı, kriz durumunda özel sektörün ve tüm toplumun destek ve işbirliğini gerekli kılmaktadır. Bu temel gereklilikler göz önünde tutulduğunda sivil hazırlıklılık açısından bazı stratejik amaçlar ön plana çıkmaktadır (CCOE t.y.):

- Devletin sürekliliğinin sağlanması ve halka temel hizmetlerin götürülebilmesi,

- Kontrolsüz halk hareketlerinin (göçlerin) önlenmesi,
- Enerji kaynaklarının güvenliği,
- Gıda güvenliği,
- Su kaynaklarının güvenliği,
- Kitlesel zayiatın önlenmesi,
- Telekomünikasyon ağının güvenliği,
- Ulaşım sistemlerinin güvenliği.

Yukarıda sıralanan stratejik maddeler modern toplumların ilk savunma hattı olarak nitelendirilmektedir. Söz konusu stratejik alanların güvenliğinin üst noktada olduğu, devlet, özel sektör ve sivil hazırlıklılığın yüksek olduğu ülkeler, dirençliliği yüksek olarak nitelendirilmektedir. Sivil direncin yüksek olduğu ülkeler olası bir kriz sonrasında daha kolay toparlanabilmektedir (Roepke ve Thankey 2019).

21. yüzyıl ulusal güvenlik anlayışı ışığında değerlendirildiğinde önleme, koruma, etkileri azaltma, yanıt verme ve hızlıca toparlanma süreçlerini birlikte yürütmeyi ifade etmektedir (FEMA 2015, 3). Terör eylemlerine ve sonuçlarına hazırlık, geniş halk kitlelerinin ve önemli tesislerin (altyapı, kimyasal-nükleer tesisler vs) terör saldırılarından alacakları zararı en aza indirmeyi amaçlamaktadır.

Güvenlikle ilgili değişen koşullar, AB ve NATO'yu toplu savunma stratejilerinde sivil hazırlıklılık vasıtasıyla direnme gücünü geliştirmeye yöneltmiştir (NATO, 2022). NATO'nun kurucu antlaşmasının 3. maddesi bu ilkeyi ortaya koyarak Müttefikleri ilkeyi yerine getirmekle yükümlü kılmış; 2016 yılında gerçekleştirilen

Varşova Zirvesi bu ilkeyi pekiştirmiştir. Ancak temel olarak sivil hazırlıklılık ulusal bir sorumluluktur. Bu konuda en iyi örnek ve planlamaları İsveç ve Finlandiya'nın gerçekleştirdiği iddia edilmektedir (Roepke ve Thankey 2019).

Avrupa Birliği hibrit tehditlerle mücadelenin merkezinde farkındalık, dirençlilik ve müdahalenin bulunduğunu kabul etmiştir. Herhangi bir tehditle mücadelede başlıca sorumluluk üye devletlere ait olmakla birlikte Avrupa Birliği, NATO ve üye devletlerin işbirliği de önemsenmektedir. Farkındalık, tehdit potansiyeli olan eylemlerin erken aşamada belirlenebilmesini amaçlamaktadır. Dirençlilik Birlik ve üye devletler dâhilindeki kurumları, toplumu ve stratejik altyapı sistemlerini korumayı amaçlamaktadır (EEAS 2018).

Avrupa Birliği 2015 yılında hibrit saldırılar ve KBRN saldırıları karşısında farkındalık ve dirençlilik oluşturmak amacıyla bazı eylem alanları belirlemiştir. Bunlar NATO'nun dirençlilik kapsamında belirlediği stratejik önerilerle benzerlik taşımaktadır. Dirençlilik ve farkındalık konusunda AB'nin belirlediği alanlardan gerçekleştirilenler ve yakın gelecekte gerçekleştirilmesi planlananlar şu şekildedir (EEAS 2018):

- Oluşturulan Avrupa Birliği Hibrit Füzyon Hücresi ile üye ülkeler ve Birlik arasında bilgi alış verişini koordine etmek, dezenformasyonu engellemek ve karşı koyma kaabiliyetini geliştirmek,
- Avrupa Birliği Hibrit Füzyon Hücresi ile toplumun dezenformasyona karşı farkındalığının ve direncinin artırılmasını sağlamak,

- Enerji kaynaklarını ve rotalarını çeşitlendirmek ve güvenlik standartlarını yükseltmek vasıtasıyla enerji sektörünün dirençliliğini artırmak,
- Ulaşımın aksamasını önlemek amacıyla önlemler almak,
- Hazırlıklılığı test etmek amacıyla Birlik çapında sağlık ve sivil koruma tatbikatları gerçekleştirmek,
- Avrupa kapsamında siber güvenliği güçlendirmek,
- Sanal dezenformasyonu engelleyerek güvenli internet ortamı oluşturmak, AB ve politikaları hakkında doğru bilgi aktarımını sağlamak,
- KBRN saldırılarına karşı hazırlıklılığı oluşturmak, bu saldırılarda kullanılabilecek maddelere erişimi kısıtlamak, bu maddelerin tedarik zincirinde yer alan özel sektör ile işbirliği geliştirerek maddelerin kullanımını sınırlandırmak, olası bir saldırıya karşı senaryolar hazırlamak,
- AB düzeyinde karşı istihbarat kapasitesini güçlendirmek; üye ülkeler, Birlik ve uluslararası kurumlar (NATO başta olmak üzere) arasında işbirliğini güçlendirmek.

AB ve NATO gibi uluslararası kuruluşların güvenlik politikalarında askeri politikaların yanı sıra dirençliliği ön plana çıkaran uygulamaları benimsediği görülmektedir. Hibrit tehditler karşısında hedef olma potansiyeli taşıyan yapıların korunması, toplumun, kurumların hazırlıklılığı önem taşımaktadır. Toplumun saldırıların oluşturacağı şok durumunu aşması ve dağılmaması için; tehdit ve saldırı sonrasında kolayca yaralarını sarması noktasında "dirençlilik" kavramı

ön plana çıkmaktadır. Sivil hazırlık ve dirençlilik halkın bu kapsamda eğitilmesini, yasal düzenlemeleri, özgür bir basını ve bu unsurların birbiriyle işbirliğini gerekli kılmaktadır (Hagelstam 2018).

Terör saldırılarına karşı hazırlıklılık, potansiyel riskleri önceden tanımlama ve etkilerini değerlendirmeyi, bu risklere yanıt verme kapasitesi inşa etmeyi ve düzenli olarak bu kapasiteyi test etmeyi içermektedir. Düzenli tatbikatlar vasıtasıyla sistemdeki açıklar test edilmeli, elde edilen veriler yeni hazırlıklılık planına dahil edilmeli ve bu süreç sürekli tekrarlanmalıdır.

Sivil hazırlıklılık aynı zamanda büyük çaplı orman yangını, sel, pandemi gibi doğal veya insan yapımı afet ve felaketlere cevap verebilme yeteneğini ifade etmektedir. Belirtilen tehdit ve tehlikeler oluşmadan önce gerekli hazırlıkların yapılması ve farkındalığın oluşturulması bu konseptin kritik bir bileşenidir (Roepke ve Thankey 2019).

Bu çalışma kapsamında aşağıdaki başlıklarda dirençlilik ve hazırlıklılık kavramları kritik altyapı ve siber alan üzerinden ele alınacak ve ulusal güvenlik üzerindeki etkileri irdelenecektir. Bu iki alanın seçilme sebebi son yıllarda küresel düzeyde yaşanan gelişmelerdir. Örneğin 2022 yılında Rusya Federasyonunun Ukrayna'ya yönelik askeri işgali sürecinde Rusya'nın ilk olarak Ukrayna'ya siber saldırıda bulunduğu ardından kritik altyapıları imha etmeye odaklandığı görülmektedir. Siber dirençlilik ve kritik altyapının dirençliliğinin önemi, iki ülke arasındaki çatışmalarda daha net açığa çıkmıştır. 4 Mart 2022 tarihinde Ruslar tarafından ele geçirilen Zaporijya Nükleer Santrali etrafında süren çatışmalar, tüm dünyayı

ciddi bir tehditle yüzyüze getirmiştir. Eylül ayında Ukrayna elektrik şebekesiyle Santralin bağlantısı tamamen kesilmiştir. Öte yandan Ağustos 2021'de Taliban'ın Afganistan'da kontrolü sağlamasının ardından Kabil'deki Uluslararası Hamid Karzai Havaalanı, ülkenin dış dünyayla hava bağlantısını sağlayan temel havaalanı olarak önemli bir işlev görmüştür. Kabil havalimanının işletmesinin ve güvenliğinin sağlanması, ülkeden tahliyelerin yapılması ve diplomatik misyonların faaliyetini sürdürmesi açısından hayati önem taşımıştır. Aşağıdaki bölümlerde kritik altyapının ve siber alanın dirençliliğinin ulusal güvenlik üzerindeki yansımaları daha detaylı olarak incelenecektir.

2. Kritik Altyapının Dirençliliği

Kritik altyapılar modern toplumların temel altyapısını oluşturan telekominikasyon sistemi, su ve enerji kaynakları, ulaştırma ve finans sistemi gibi yapılardır. Bu altyapıların herhangi birinde oluşacak bir kesinti vatandaşların refahı ve ekonomi üzerinde olumsuz etkilere sebep olacaktır. Doğal afetler, endüstriyel kazalar, terörist saldırılar, siber saldırılar kritik altyapıların güvenliği açısından dikkate alınması gereken tehditlerdir (OECD 2019). Kritik altyapılar genel olarak belirli bir saldırı veya doğal afette direncin ilk basamağı olarak nitelendirilmektedirler. İlk şok dalgası tehditin ilk oluştuğu zaman dilimi olup, fiziksel dayanıklılık ve diğer güvenlik sistemleri ile beraber dirençliliğin ilk aşaması olarak kabul edilmektedir (Ersavaş Kavanoz 2021, 386).

Birleşmiş Milletler Afet Riski Azaltma Ofisi (UNISDR) kritik altyapı kavramını "gerek olağan şartlar altında gerekse olağanüstü acil durum şartlarında toplumun işleyişi bakımından sosyal, ekonomik veya

operasyonel anlamda hayati önem taşıyan temel fiziksel yapılar, teknik tesisler ve sistemler" olarak tanımlamıştır. Amerika Birleşik Devletleri Ulusal Güvenlik Sekreterliğinin yaptığı tanım ise şu şekildedir: "Birleşik Devletler için, fonksiyonelliğini yitirmesi veya tahrip olması durumunda devletin güvenliği, ulusal ekonominin güvenliği, kamu sağlığı ve güvenliği ya da bunların birden fazlası açısından sarsıcı etkiler doğuracak derecede hayati olan fiziki veya sanal sistemler ve varlıklar." (Connell vd. 2018, 6).

Kritik altyapı kavramını AFAD (Afet ve Acil Durum Yönetimi Başkanlığı) şu şekilde tanımlanmaktadır (2014, 4): "İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür." Bütün bu tanımlardan ortaya çıkan sonuç, kritik altyapının güvenliğinin sağlanmasının kamu güvenliği, ulusal güvenlik, halk sağlığı, toplum refahı, ekonomik refah üzerinde doğrudan etkisi olduğudur. Kritik altyapılar fiziki yapılar olabildiği gibi sanal sistemler de olabilmektedir. Söz konusu altyapıların inşaası büyük maliyetler gerektirmekte olup bu sistemlerin kesintiye uğramasının maliyeti kat kat fazla olabilmektedir. Bu durumun bir sebebi de karşılıklı bağımlılıktır. Buna göre farklı altyapı sektörlerinden birinde görülecek kesinti diğer altyapıları da etkileyecektir (CISA 2019, 4).

Kritik altyapıların dirençliliği, bireysel ve kamusal hayatın devamı için gerekli ulaşım, iletişim, haberleşme, enerji, su, finans gibi sektörlerin sürekliliğini sağlamayı amaçlamaktadır. Belirtilen alanlardaki tehdit ve açıkları önceden belirlemek, olası bir tehdit ve

saldırı anında sürekliliği sağlamak veya en az hasarla süreci atlatmak için önlemler almak, saldırı veya kaza sonrasında hızlı bir şekilde sistemin onarımını sağlamak, değişen koşullara uyum sağlamak sistemin direncini belirtmektedir (OECD 2019).

Kritik altyapının dirençliliği can ve mal kaybı ile ekonomik zararın engellenmesi, kamu düzeninin sağlanması ve ulusal-bölgesel güvenlik açısından önem arz etmektedir. Kritik altyapılar şu şekilde sıralanabilir (Ünver, Canbay ve Özkan 2011):

- Tarım ve gıda sektörü,
- Kimyasal tesisler,
- Bankacılık ve finans sistemi,
- Ticari tesisler,
- Su sistemleri (barajlar, depolama, dağıtım),
- Bilgi ve iletişim,
- Acil servisler, hükümet binaları,
- Ulusal anıtlar,
- Nükleer reaktörler, elektrik, gaz, rafineriler,
- Posta, nakliye ve ulaşım sistemi (havaalanları, demir yolları, trafik kontrol sistemleri).

Avrupa Birliği ve çeşitli ülkelerin kritik altyapılara ilişkin kategorilendirmeleri bulunmaktadır. Kaybı veya zarar görmesi halinde ortaya çıkacak etkiler en düşükten en fazlaya doğru kategorilendirilmektedir. En yüksek önceliğe sahip altyapıların sayıca az olması gerektiği ifade edilmektedir. Bu kategorideki altyapılar, kaybı

halinde uzun süreli ulusal etkileri olacak, birden fazla sektörü etkileyecek ulusal öneme sahip varlıklardır (Connell vd. 2018, 6).

21. yüzyılda değişen risk tanımları ve buna bağlı olarak değişen güvenlik algısı, kritik altyapının dirençliliğini sağlamak için hazırlıklı olmayı gerekli kılmaktadır. Herhangi bir doğal afet neticesinde oluşan altyapı hasarı doğal afetin kendisinden daha fazla zarara yol açabilmekte, toparlanmayı güçleştirmekte, psikolojik, ekonomik ve sosyal tahribatlara sebep olmaktadır. Kuvvetli fırtınalar elektrik iletim sistemleri üzerinde zararlar oluşturabilmekte, depremler yollar ve köprülerin yıkılmasına sebep olmakta, pandemiler sağlık sistemini çökertmekte, siber saldırılar internet altyapısını hedef almakta ve terör saldırıları nükleer tesisler, enerji santralleri vb. altyapıları hedef olarak seçebilmektedir.

Örneğin 2011 yılında gerçekleşen deprem ve ardından gerçekleşen tsunami felaketi neticesinde Japonya'nın enerji sektörü darbe almıştır. Depremin merkez üssüne 180 km uzaklıktaki Fukushima Daiichi Nükleer Santraline tsunami dalgalarının ulaşmasının ardından santralde ciddi hasarlar ortaya çıkmıştır. Santralden havaya salınan radyasyon sebebiyle santralin çevresindeki 20 km alanda tahliyeler yapılmaya başlanmıştır. Santrale giden yolların da zarar görmesi sebebiyle dışarıdan müdahale güçlükle yapılmıştır (AFAD t.y.). Bir başka örnek olarak 2012 yılında Atlantik'te oluşan Sandy Kasırgası, bu bölgede kayıtlara geçen en büyük kasırga olmuştur. Kasırga ABD, Kanada, Jamaika, Haiti ve Küba'yı etkilemiştir. Bu afet sonrasında ABD'nin doğusunda uzun süreli elektrik kesintisi oluşmuş, metro hatları haftalarca çalışamamıştır. 5.4 milyon aracın mahsur kalması, kasırganın kendisinden daha fazla miktarda iş hayatını zarara

uğratmıştır. Kasırga neticesinde 8.5 milyon haneye elektrik sağlanamamıştır. 2010 yılında İzlanda'da yer alan Eyjafjallajökull Yanardağının patlaması sonucunda Avrupa hava sahası kapatılmış ve 100.000'den fazla uçuş iptal edilmiş veya yönlendirilmiştir. Kargo uçuşları da etkilendiği için tedarik ve üretim sistemi ciddi zarar görmüştür (OECD 2019). Bu ve benzeri örnekler kriz ve şoklar karşısında altyapıda oluşan hasarın etkilerinin büyüklüğünü gözler önüne sermektedir. Altyapı hasarları nedeniyle insanların haftalarca elektriksiz kalması, internet erişiminin olmaması, yakıt ve doğalgaz, su ve gıdaya ulaşamaması, yolların ulaşıma elverişli olmaması toplumda büyük bir panik ve kaos oluşturmaktadır. Özellikle terör saldırıları sonrasında altyapı hasarıyla beraber oluşan panik duygusu, saldırının amacına ulaşması anlamına da gelmektedir.

Kritik altyapıların korunmasının önemine ilk olarak 1997 yılında ABD'de yayınlanan bir raporla dikkat çekilmiştir. Ardından çıkarılan bir direktif, kritik altyapı ile ilgisi bulunan özel sektör ve kamu kuruluşlarına gönderilmiştir. 2006 yılında hazırlanan Kritik Altyapı Görev Gücü (CITF) Raporunda raporun hazırlanma amacı, kritik altyapının daha dirençli hale getirilmesi için ulusal siyasa ve stratejiler oluşturulması şeklinde belirtilmiştir. Siber veya fiziki altyapıların korunmasının Birleşik Devletlerin iç güvenlik stratejilerindeki her türlü hazırlıklılık planının temelinde yer alması gerektiği vurgulanmıştır (US HSAC 2006, iii).

Kritik Altyapı Görev Gücü raporunda kritik altyapı koruma (CIP) kavramının zayıf bir strateji olduğuna ve tek tek bütün potansiyel hedeflerin çeşitli saldırılardan korunmasının güçlüğüne vurgu yapılmaktadır. Buna göre koruma kavramının kendisi ölçülebilir

değildir ve kritik altyapılar için sağlanacak korumanın ne oranda yeterli olacağı belirsizdir. Raporda kritik altyapı koruma kavramı yerine kritik altyapı dirençliliği (CIR) kavramı önerilmektedir. Buna göre dirençlilik ölçülebilir, objektif amaçlar vermekte, herhangi bir şok ve kriz sürecinde sistemin bütün fonksiyonlarıyla tekrar çalışabilmesi için gerekli zamanı önceden tayin edebilmektedir. Raporda dirençlilik "bir sistemin içsel ve dışsal değişiklikler karşısında kendi fonksiyonlarını ve yapısını devam ettirebilme kapasitesi" olarak tanımlanmaktadır. Kritik altyapı direnci için gerekli bir faktör olarak psikolojik dirence de dikkat çekilmiştir. Kritik altyapının herhangi bir felaketten kendini kurtarma yeteneği aynı zamanda sistemin kullanıcılarının hareketlerine, bilincine ve değişen güvenlik ortamına uyum sağlayabilmesine de bağlıdır (US HSAC 2006, 5). Bu durum kritik altyapı dirençliliğinde, eğitimin ve önceden hazırlıklılığın önemine vurgu yapmaktadır.

Avrupa Birliği ise Madrid ve Londra'da tren ve metro istasyonlarına yapılan saldırılar sonrasında konuyu gündeme almış ve altyapılara yönelik saldırılara karşı hazırlıklı olunması politikasını benimsemiştir. 2004 yılında yayınlanan "Terörle Mücadele için Kritik Altyapı Korunması" başlıklı rapor ile Birlik için kritik altyapıların önemi vurgulanmıştır (Lindström ve Olsson 2009, 37). 11 Eylül ve sonrasında terör örgütlerinin özellikle büyük şehirleri ve metro gibi ulaşım ağlarını hedef alması, ulusal güvenlik kapsamında kritik altyapının dirençliliğinin önemini ortaya koymaktadır.

AB 2004 yılında Kritik Altyapıların Korunması için Avrupa Programı (EPCIP)'nı geliştirmiştir. Ardından Kritik Altyapılar Uyarı Bilgi Ağı (CIWIN) oluşturulmuştur. 2008 yılında Avrupa Kritik Altyapıların Belirlenmesi ve Koruyucu Tedbirlerin Artırılması direktifi

yayınlanmıştır. AB kritik altyapıların zarar görebilirliğini azaltmayı ve dirençliliğini artırmayı temel görevleri arasında görmektedir. Terör eylemleri, yanlış uygulamalar veya doğal afetler neticesinde kritik altyapının zarar görmesi hem AB'nin güvenliği hem de vatandaşların refahı açısından olumsuz neticeler doğuracaktır. AB bünyesinde bu konuda çalışan Terörizm ve Güvenlikle Alakalı Diğer Risklerin Önlenmesi, Hazırlıklılık ve Sonuç Yönetimi Komitesi oluşturulmuştur. Bu program kapsamında 2007-2012 döneminde 100 farklı projeye mali destek verilmiştir. Projeler neticesinde AB vatandaşlarının ve kritik altyapıların terörist saldırılardan ve diğer güvenlikle alakalı kazalardan korunması ve hazırlıklılığın sağlanması amaçlanmıştır (European Commission 2022).

Türkiye'de kritik altyapının korunmasına ilişkin özel bir stratejik planın bulunmadığı ancak Resmi Gazetede yayınlanan kararlar ve yönetmeliklerle konunun usul ve esaslarının düzenlendiği ifade edilmektedir. TÜBİTAK'ın hazırladığı "Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı" Türkiye'deki kritik altyapıları tanımlamış ve asgari güvenlik önlemlerini belirtmiştir (Genco 2020, 41).

Türkiye üzerinden pek çok kıtalararası enerji hattı geçmektedir. Türkiye aynı zamanda deprem fay hatları üzerinde yer almaktadır. Diğer yandan ülkedeki terörist unsurlar ve istikrarsız/kırılgan ülkelere yakınlığı kritik altyapılara yönelik olası terör eylemlerini düşünmesini ve stratejik planlar yapmasını gerekli kılmaktadır. Türkiye'nin konumu, kritik altyapılardaki bir tehlikenin pek çok ülkeyi de etkilemesine yol açabilecektir.

Kritik altyapıların güvenliğini ulusal güvenlik bağlamında ele almak bir zorunluluktur. Afet yardım ve acil durum yönetiminin yanı sıra kritik altyapılara terör saldırıları ve siber saldırıda bulunulabileceği düşünülerek önlemler geliştirilmesi gerekmektedir. Pek çok örnekte kritik altyapıların mülkiyetinin özel sektörde olduğu veya üretim ve dağıtım hizmetinin özel sektör eliyle yürütüldüğü görülmektedir. Bu durumda özel ve kamu işbirliğinin sürdürülmesi ulusal güvenlik açısından şart olmaktadır. Diğer yandan birden fazla ülkeyi ilgilendiren kritik altyapılar için bölgesel ve uluslararası işbirliği de gerekmektedir (Ak 2019, 50).

Özellikle kritik alanlarda faaliyet gösteren özel işletmelerin dirençliliği ve olası bir tehdit karşısında devletin bu işletmeler üzerinde koordinasyonu sağlaması önem taşımaktadır. Yine bu kapsamda, enerji, telekomünikasyon, ulaşım, limanlar gibi kritik sektör ve alanlarda yabancı mülkiyeti, kriz anında devletin bu altyapıya erişimini ve kontrolünü etkileyecektir. Özellikle askeri unsurların desteklenmesi gerektiği kriz durumlarında, ulusal dirençlilik açısından kritik alanlarda kontrol ve koordinasyonun sağlanması önemli görülmektedir (Roepke ve Thankey 2019). Kritik altyapının dirençliliğinin ulusal güvenlik kapasitesi ile doğru orantılı olduğu ortaya çıkmaktadır. Kritik altyapının direncini arttırmak için özel sektör, kamu kuruluşları ve sivil toplum örgütlerinin işbirliğini içeren tüm devlet ve tüm toplum yaklaşımının benimsenmesi gerektiği görülmektedir.

3. Siber Tehditlere Karşı Hazırlıklılık

Siber tehditlere karşı hazırlıklılık, siber tehditleri tanımlamayı, önlemeyi ve yanıt vermeyi kapsamaktadır. Günümüzde ülkelerin

ekonomik büyümeleri bilgi ve iletişim teknolojilerine sıkı sıkıya bağlıdır. Devletler üretkenliği ve etkinliği artırmak, ekonomik kalkınmaya katkıda bulunmak amacıyla e-devlet, e-bankacılık, dijital sağlık ve dijital eğitim gibi alanlara daha fazla yatırım yapmaya başlamıştır. Yapılan araştırmalar, bilgi ve iletişim teknolojilerindeki gelişmelerin devletlerin ekonomik kalkınmalarına ciddi katkılarda bulunduğunu göstermektedir. Ancak bu teknolojilerde kesintiler yaşanması mümkündür. Bilgi ve iletişim teknolojilerinde gerçekleşen kesintiler sonucu ekonomik anlamda kayıplar yaşanmaktadır (Hathaway 2013). Siber güvenliğin kamu hizmetleri, sağlık, eğitim, ulaşım vb. pek çok alanla yakından ilişkisi, siber dirençliliği kamusal güvenliğin bir parçası haline getirmektedir. Siber güvenlik açıkları can kayıplarına yol açabilmekte, sisteme güveni sarsabilmekte ve finansal piyasalarda istikrarsızlığa yol açabilmektedir (Seren 2016, 13).

Siber güvenliğin sağlanması amacıyla elektrik şebekeleri, finansal sistemler, havacılık, enerji santralleri, sağlık sistemleri, ulaşım sistemleri gibi siber yaşam alanlarında tüm sayılan sistemlere özgü ulusal stratejiler hazırlanması esastır. Diğer yandan teknolojik altyapıların sivil ve askeri maksatlarla kullanılması, bu sistemlere yönelik bir saldırının siber savaş olarak tanımlanmasına yol açacaktır (Seren 2016, 13).

Siber tehditlere karşı hazırlık, devletlerin ulusal siber güvenlik stratejisi oluşturması ve yayınlamasını, operasyonel birimler oluşturmasını, siber güvenlik alanında ulusal ve uluslararası işbirliği içerisinde olmasını, siber tehditlere karşı caydırıcı ve cezalandırıcı politikalar geliştirmesini, siber güvenlik alanında araştırma ve geliştirme fonlarına yatırım yapmasını gerektirmektedir (Hathaway

2013).

Küresel düzeyde siber güvenliği sağlamaya yönelik ortak standartlar kabul edilmiştir. Bilgi Güvenliği Yönetim Sistemleri ve Bilgi Teknolojileri Güvenliği için Değerlendirme Kriterleri, küresel düzeydeki düzenlemelerdir. Diğer yandan siber güvenliği sağlamak amacıyla Avrupa Birliği ve NATO düzeyinde de kriterler geliştirilmiştir (Ünver, Canbay ve Mirzaoğlu 2009, 34-5).

NATO siber alanı, kara, hava, deniz ve uzaydan sonra beşinci savaş alanı olarak kabul etmiştir. Siber saldırılara karşı önlem alınması NATO'nun gündemine ilk olarak 2002 yılında Prag'da yapılan zirve toplantısında girmiştir. NATO 2008 yılında ilk siber savunma politikasını benimsemiş, 2014 yılında ise, toplu savunma politikasının bir parçası olarak kabul etmiştir. Toplu savunma politikası kapsamında herhangi bir siber saldırının NATO'nun kuruluş antlaşmasındaki en önemli maddelerden olan 5. maddeyi devreye sokmasıyla sonuçlanacağı kabul edilmiştir (Brent 2019).

Avrupa Birliği bünyesinde siber suçlara karşı mücadele amaçlı Avrupa Şebeke ve Bilgi Güvenliği Ajansı (ENISA), Bilgisayar Acil Müdahale Ekibi (CERT) ile Avrupa Siber Suç Merkezi (EC3) oluşturulmuştur. Birleşmiş Milletler bünyesinde ise bu amaçla faaliyet gösteren GGE – Birleşmiş Milletler Hükümet Uzmanları Grubu bulunmaktadır (Bendiek ve Maat 2019; BTK 2022, 36, 39).

Türkiye ise 2010 yılında Avrupa Konseyi Siber Suçlar Sözleşmesine taraf olmuş, 2012 yılında Siber Güvenlik Kurulunu oluşturmuştur. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014

Eylem Planının ardından 73 kurum ve kuruluştan uzmanın katılımıyla 2016-2019 Ulusal Siber Güvenlik Stratejisi oluşturulmuştur. TÜBİTAK bünyesinde Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi, EGM bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı oluşturulmuştur. Askeri alanda ise Genelkurmay Başkanlığına bağlı Siber Savunma Komutanlığı bulunmaktadır. 2017 yılında kamu kurumları, akademisyenler ve özel sektörün katılımıyla Türkiye Siber Güvenlik Kümelenmesi oluşturulmuştur (Aldemir ve Kaya 2020, 17; Mataracıoğlu vd. 2020, 918-919).

Siber güvenliği sağlamada tek başına kamu kurum ve kuruluşları veya özel sektörün yeterli olamayacağı belirtilmektedir. Siber alanın güvenliği, bireyleri, ekonomiyi, altyapı sistemlerini, askeri güvenliği ve özel sektörü de etkileyen bir niteliğe sahiptir. Bu durum kamu-özel sektör, üniversite ve sivil toplumun işbirliğini gerekli kılmaktadır. STK'lar vatandaşların kendi güvenliklerinin farkındalığını artırmaya, üniversiteler siber güvenlik alanında araştırma ve geliştirme faaliyetlerini desteklemeye, özel sektör uzmanlık, bilgi ve birikimi ile tedbirler almaya katkıda bulunmalıdır. Kamu sektörü ise yasal mevzuat ve standartlar oluşturarak düzenleyici rol oynamalıdır (Ünver, Canbay ve Mirzaoğlu 2009, 38). Nitekim 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında (TC Ulaştırma ve Altyapı Bakanlığı, 30), eylem planının paydaşları "kamu kurum ve kuruluşları, kritik altyapılarda faaliyet gösterenler başta olmak üzere özel sektör kurum ve kuruluşları, üniversiteler, sivil toplum kuruluşları, araştırma toplulukları ve ülkemizdeki bireyler ile uluslararası paydaşlar" olarak sıralanmıştır. Böylelikle siber dirençliliğin sağlanmasında tüm toplum ve tüm devlet yaklaşımının önemi ortaya çıkmaktadır.

Ulaştırma ve Altyapı Bakanlığı tarafından TÜBİTAK'a hazırlatılan "Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı"nda bilişim sistemlerinde uyulması gereken asgari güvenlik standartları belirlenmeye çalışılmıştır. Raporda kritik altyapı kapsamında değerlendirilen bilişim sistemlerinin bilgi sistemleri ve iletişim sistemleri olarak ikiye ayrıldığı belirtilmiştir. Kritik altyapılar hizmet vermek için Endüstriyel Kontrol Sistemleri (EKS) ve bilişim sistemlerini kullanmaktadırlar. EKS ise SCADA ve Dağınık Kontrol Sistemleri olarak ikiye ayrılmaktadır. Dolayısıyla raporda kritik altyapı bilgi sistemleri dört kategoride ele alınmıştır (TÜBİTAK, 6):

- Bilgi Sistemleri, bir kuruma hizmet veren bilgisayar sistemlerini,
- İletişim Sistemleri, geniş bir alanda hizmet veren birden fazla kurum ve kuruluşa iletişim hizmeti sağlayan sistemleri,
- SCADA Sistemleri, geniş bir alana yayılmış bir sistemin merkezi olarak izlenmesi ve kontrolünü sağlayan sistemleri,
- Dağınık Kontrol Sistemleri, belirli bir tesis ve konumla sınırlı bir endüstriyel sürecin kontrolünü sağlamak için tesis içinde kullanılan sistemleri ifade etmektedir.

Rapora göre kritik altyapı bilgi sistemlerinin asgari güvenliği açısından dikkat edilmesi gereken önlemler şu şekilde özetlenebilir (TÜBİTAK, 10-16):

- Sistemlere yetkisiz erişimin engellenmesi gerekmektedir. Bu amaçla sistem merkezine fiziksel giriş ve çıkışlar takip

edilmeli, buraya girebilecek personel sınırlı tutulmalı ve kayıt altına alınmalıdır. Diğer yandan Endüstriyel Kontrol Sistemleri İntranet/Ekstranetten izole edilmeli, sisteme ağ üzerinden erişim engellenmelidir. EKS'ye taşınabilir saklama ortamlarının bağlanmaması için önlem alınmalıdır.

- Yetkili personelin sistemlere erişiminin kontrolü sağlanmalıdır. Bu amaçla EKS'lerde görevli personelin güvenlik geçmişi iyi araştırılmalıdır. Özellikle sistem yöneticisi atamalarında titiz davranılmalıdır. Yetkili personelin sisteme erişmek için kullanıcı kimlikleri ve parolaları kullanarak güvenli oturum açmaları sağlanmalıdır.
- Yetkili personel ve sistem yöneticilerinin yaptığı işlemler kayıt altına alınmalıdır.
- Sistem yöneticisi ve operatör gibi roller iyi tanımlanmalı, bu görevlilere verilen roller ve sorumluluklar net olarak tanımlanmalıdır.
- EKS ve bilişim sistemlerinde uygulama yazılımlarının güvenliği sağlanmalıdır.
- EKS ve bilişim sistemlerinde sistem merkezinin devre dışı kalması ihtimaline karşı yedek sistem merkezi oluşturulmalı ve gerektiğinde devreye girmesi sağlanmalıdır.
- Kritik altyapı sistemlerinde personel sürekliliği sağlanması güvenlik açısından önemlidir. Diğer yandan gerekli personelin yetiştirilmesine de önem verilmelidir.
- Kritik altyapı sistemlerinde yukarıda sıralanan güvenlik

önlemleri uygulanırken aynı zamanda kayıt tutulması da gerekmektedir. Bu kayıtlar delil niteliğinde olup matbu veya elektronik olabilirler. Kayıtların kurum içi ve kurum dışı denetçiler tarafından değerlendirilmesi sağlanmalıdır.

Siber tehditlere hazırlık kapsamında, herhangi bir saldırı öncesinde risk değerlendirmesi yapılması önemlidir. Risk değerlendirmesi, tehditleri saptamayı ve saptanan riskleri bertaraf etmenin yollarını belirlemeyi içermektedir. Siber güvenlik risk değerlendirmesi, dijital dünyayla ilişkili her kişi ve kuruluşu kapsamaktadır. Siber güvenlikle ilgili atılan her adımda siber risklerin de değiştiği ve geliştiği kabul edilmektedir. Hatta hiçbir ülkenin siber risklere karşı tamamen hazırlıklı olmadığı da dile getirilmektedir (Hathaway, Demchak vd. 2015).

Siber saldırı ve tehditlere karşı uluslararası kuruluşların, devletlerin ve özel kuruluşların hazırlıklılığı kadar bireylerin hazırlıklılığı da önemlidir. Çünkü saldırganlar bireylerin özel, finansal ya da sağlık bilgilerini çalmayı amaçlıyor olabilirler. Kişisel bilgisayarlara, telefonlara erişerek bu bilgilere sahip olmak, kişisel saygınlığa, finansal güvenliğe zarar vermek, kimlik bilgileri ile hırsızlık yapmak saldırganların hedefleri arasında olabilir. Bu ihtimalleri en aza indirmek üzere bireysel önlemler almak da önem taşımaktadır. Bireylerin siber saldırı türlerini bilmesi ve bu saldırılara yönelik farkındalık oluşturması ile mahremiyet artırıcı teknolojileri, elektronik imza ve akıllı kartları kullanması kişisel güvenliği artırıcı tedbirler arasında yer almaktadır (Yılmaz 2014-15, 49). Terör saldırıları ve diğer hibrit tehditler sırasında veya savaşlar esnasında doğrudan ve öncelikli olarak siber güvenliğin hedeflenmesi siber hazırlık ve dirençliliğin

ulusal güvenlik üzerindeki doğrudan etkisini ortaya çıkarmaktadır. Siber hazırlıklılık ve dirençliliğin toplumdaki tüm aktörlerin doğrudan katılımıyla sağlanabileceği anlaşılmaktadır.

Sonuç

Günümüz koşullarında ulusal güvenliğe yönelik tehditlerin çeşitlenen doğası, ülkeleri çok yönlü tedbirler almaya yöneltmiştir. Tehditlerin önceden belirlenerek tehdit sırasında izlenmesi gereken adımların belirlenmesi ve tehdit sona erdikten sonra sistemin hızlıca toparlanmasının sağlanması, sistemin dirençlilik seviyesini göstermektedir. Dirençli bir toplum oluşturmanın yolu ise hazırlıklılıktan geçmektedir.

Hazırlıklılık yoluyla dirençlilik, ulusal güvenlik tanımının bir parçası durumuna gelmiştir. Mikro ve makro düzeyde dirençlilik planları yapılması, olası bir kriz durumunu atlatmanın ve oluşacak hasarları en kısa sürede gidererek sisteme işlerlik kazandırmanın etkili bir yoludur. Bu amaçla hayatın pek çok alanını etkileyen, askeri sistemlerin de faaliyetlerini sürdürmesi için gerekli olan siber dirençlilik ile kritik altyapı dirençliliğinin ön plana çıktığı görülmektedir.

Bu çalışmada kritik altyapının ve siber alanın dirençliliğinin ulusal güvenliğin tesisinde ağırlıklı bir rolü olduğu sonucuna ulaşılmıştır. Ulaşılan sonuçlardan bir diğeri ise gerek kritik altyapı gerekse de siber dirençlilik kapsamında bireyler, kurumlar, özel sektör, üniversiteler, topluluklar ve sivil toplum örgütlerini de kapsayan ve gerektiğinde uluslararası işbirliğini de içeren bütüncül bir yaklaşımın benimsenmesinin zorunluluğudur.

KAYNAKÇA

(CCOE) Civil-Military Cooperation Centre of Excellence. t.y. Resilience Through Civil Preparedness. The Hague: A CCOE Info Sheet.

AFAD. 2014. *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*.

AFAD. t.y. "Fukushima Daiichi Nükleer Santral Kazası." Erişim: 05.05.2022. www.afad.gov.tr/kbrn/fukushima-daiichi-nukleer-santral-kazasi.

Ak, Tarık. 2019. "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması." *ASSAM Uluslararası Hakemli Dergi* (1): 42-51.

Aldemir, Ceray ve Merve Kaya. 2020. "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları." *Kamu Yönetimi ve Uygulamaları Dergisi* 1(1): 6-27.

Bendiek, Annegret ve Eva Pander Maat. 2019. "The EU's Regulatory Approach to Cyber-security." *German Institute for International and Security Affairs*, Research Division EU Working Paper.

Brent, Laura. 2019. "NATO'nun Siber Uzaydaki Rolü." *NATO Review*. Şubat 12, 2019. https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydaki-rolue/index.html.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). 2022. *Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri.*

CISA (Cyber and Infrastructure). 2019. A *Guide to Critical Infrastructure Security and Resilience.*

Coaffee, Jon. 2009. *Terrorism, Risk and the Global City Towards Urban Resilience*. Farnham: Ashgate Publishing.

Connell, Richenda, Benjamin Rabb, Mehmet Kemal Demirkol, Federico Carturan, Dilek Özceylan Aubrecht, Arif Cem Gündoğan, Mustafa Erdik, Burcu Özçam Adıva, Sinan Akkar,

Oguz Bagis, Bob Khosa, Serena Odianose, Virginie Fayolle ve Sophie Turner. 2018. *Çukurova Kritik Altyapı Risk Değerlendirme (CIRA) Projesi*. Washington DC: Dünya Bankası.

Dupuy, Arnold C., Dan Nussbaum, Vytautas Butrimas, Alkman Granitsas. 2021. "Energy Security in the Era of Hybrid Warfare". *NATO Review*, Ocak 13, 2021. www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.

EEAS (European External Action Service/Avrupa Dış Eylem Servisi). 2018. "A Europe that Protects: Countering Hybrid Threats." Haziran 13, 2018. https://eeas.europa.eu/node/46393_en.

Ersavaş Kavanoz, Suna. 2021. "Kentsel Direnç Planlamasında İş Birliği." *Erciyes Üniversitesi İİBF Dergisi* 59 (Mayıs-Ağustos): 375-390.

European Commission. "Critical Infrastructure." European Commission Migration and Home Affairs. Erişim: 05.05.2022. https://ec.europa.eu/home-affairs/pages/page/critical-infrastructure_en.

FEMA. 2015. *National Preparedness Goal*. U.S. Department of Homeland Security Federal Emergency Management Agency.

Genco, Abdullah. 2020. "Türkiye'de Kritik Altyapı ve Kritik Altyapıya Yönelik Tehditler." *KAYTEK Dergisi* 2(2): 38-46.

Hagelstam, Axel. 2018. "Cooperating to Counter Hybrid Threats." *NATO Review*, November 13, 2018. www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri. 2015. "Cyber Readiness Index 2.0." November 30, 2015. www.belfercenter.org/publication/cyber-readiness-index-20.

Hathaway, Melissa. 2013. "Cyber Readiness Index 1.0." Belfer Center November 8, 2013. www.belfercenter.org/publication/cyber-readiness-index-10.

Jore, Sissel H. 2020. "Is Resilience a Good Concept in Terrorism Research? A Conceptual Adequacy Analysis of Terrorism Resilience." *Studies in Conflict & Terrorism* 46 (1): 1-20.

Kindt, Michael T. 2006. "Building Population Resilience to Terror Attacks: Unlearned Lessons from Military and Civilian Experience". *The Counterproliferation Papers Future Warfare Series* No: 36. Alabama: Air University.

Lindström, M. ve S. Olsson. 2009. "The European Programme for Critical Infrastructure Protection." In *Crisis Management in the European Union*, derleyen S. Olsson, 37-59. Berlin, Heidelberg: Springer.

Mataracıoğlu Tolga, K. C. Kalıpcıoğlu, S. M. Arıkan, G. Işık, Y. Demiral, D. Cincioğlu ve H. A. Mantar. 2020. "Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği". *Küresel Salgının Anatomisi İnsan ve Toplumun Geleceği*, derleyen M. Şeker, A. Özer ve C. Korkut, 911-940. Ankara: TÜBA.

NATO. "Resilience, civil preparedness and Article 3." Erişim: 20.08.2022. www.nato.int/cps/en/natohq/topics_132722.htm.

Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, Rose L. Pfefferbaum. 2008. "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness." *American Journal of Community Psychology* 41: 127-150.

OECD. 2019. "Good Governance for Critical Infrastructure Resilience." *OECD Reviews of Risk Management Policies*, June 2019.

Roepke, Wolf Diether ve Thankey, Hasit. 2019. "Direnme Gücü: Savunmanın İlk Hattı". *NATO Review*, Şubat 29, 2019. www.nato.int/docu/review/tr/articles/2019/02/27/direnme-guecue-savunmanin-ilk-hatti/index.html.

Seren, Merve. 2016. "Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık." *SETA* 183 (Aralık).

TÜBİTAK. t.y. *Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı.*

US HSAC (Homeland Security Advisory Council). 2006. *Report of the Critical Infrastructure Task Force.*

Ünver, Mustafa, Cafer Canbay ve Ayşe Gül Mirzaoğlu. 2009. *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Ünver, Mustafa, Cafer Canbay ve Hüseyin B. Özkan. 2011. *Kritik Altyapıların Korunması.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Varol, Nehir ve Esma B. Kırıkkaya. 2017. "Afetler Karşısında Toplum Dirençliliği." *Dirençlilik Dergisi* 1(1): 1-9.

Wıgell, Mikael, Harri Mıkkola, Tapio Juntunen. 2021. *Best Practices in the whole-of-society approachin countering hybrid threats.* European Pariament Coordinator: Policy Department for External Relations.

Yılmaz, Hasan. 2014-15. "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi". *Denetişim* (15): 45-59.